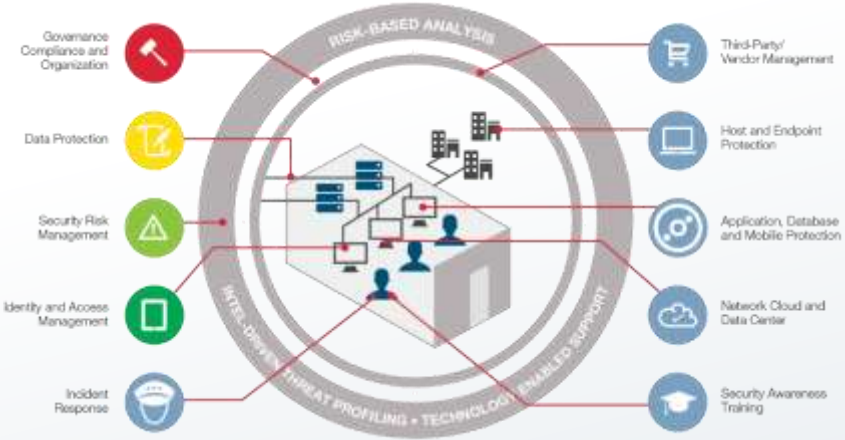
InfosecPartners
CYBERSECURITY

Security Risk Assessment

Security Consulting Services by Infosec Partners
March 2016 | Francisco Ordillano

How Prepared Are You?

*A **Security Risk Assessment** "allows organisations to assess, identify and modify their overall security posture and enables security, operations, organisational management and other personnel to collaborate and view the entire organization from an attacker's perspective." (ISACA)*



Reasons for a Security Risk Assessment

- » Legal & Regulatory Requirements
- » Cost Justification & Productivity
- » Communication & Breaking Barriers

Security Risk Assessment – What you get

- **Executive Summary**

  A summary of findings and recommendations along with key benchmarking insights.

- **Observations and Gap Analysis**

  Using industry frameworks as a benchmark, the gap analysis identifies domains that need further development and provides a maturity development plan to help strengthen security posture and reduce risk.

- **Security Program Roadmap and Recommendations**

  A strategic and tactical plan with recommendations on sequencing and prioritisation for improving the effectiveness across domains.

Security Risk Assessment - Stages

1. Crown Jewels Analysis

- Classification of data assets.
- Which are mission critical/high value?
- Which resources are most important?

2. Threat Susceptibility

Specific to the organisation:

- What threats are being faced?
- What are the vulnerabilities?

3. Risk Remediation

- How are risks currently mitigated?
- What controls are in place?
- What changes are in the pipeline?

4. Gap Analysis

Specific to the organisation:

- What is the Risk Appetite?
- Are current controls sufficient?

5. Strategy & Planning

- Address critical areas
- Define priorities
- Agree strategy, schedule & budget

1. Crown Jewels Analysis

"Identifies cyber assets that are most critical to the accomplishment of an organisation's mission."

Enterprise Critical	Critical intellectual property. Top-secret plans & formulas.
Executive	Acquisition/ divestiture plans. Executive/board deliberations.
Regulated	SPI & PII. Quarterly results. PCI-DSS. Data Protection. Sarbanes-Oxley.
Business Strategic	External audit results. Alliances & JV partner data. Business strategic plans.
Business Unit Critical	Design documents. R&D results. Customer records. Pricing data. Security data.
Operational	Project plans. Contracts. Salaries & benefits data. Accounts receivable.
Near-Public	List of partners. Revenue growth by segments. Market intelligence. Pay comparison data.

Crown Jewels
0.01-2.0%

2. Threat Susceptibility Assessment

"Evaluates the susceptibility of an organisation to threats and vulnerabilities."

VULNERABILITIES	THREATS	FACTORS
» Careless or unaware employees » Unauthorised access » Outdated security controls or architecture » Related to Cloud » Related to Mobile » Related to Social Media	» Cyber attacks to steal data e.g. intellectual property, financial information » Internal attacks e.g. disgruntled employees » Cyber attacks to disrupt/deface organisation » Fraud, Phishing, Social Engineering » Zero-day, Malware, Ransomware, DDoS » Advanced Persistent Threats	» Proximity » Recovery time » Impact (CIA) » Required skills » Stealth » Locality » Restoration cost » Prior use » Required resources » Attribution

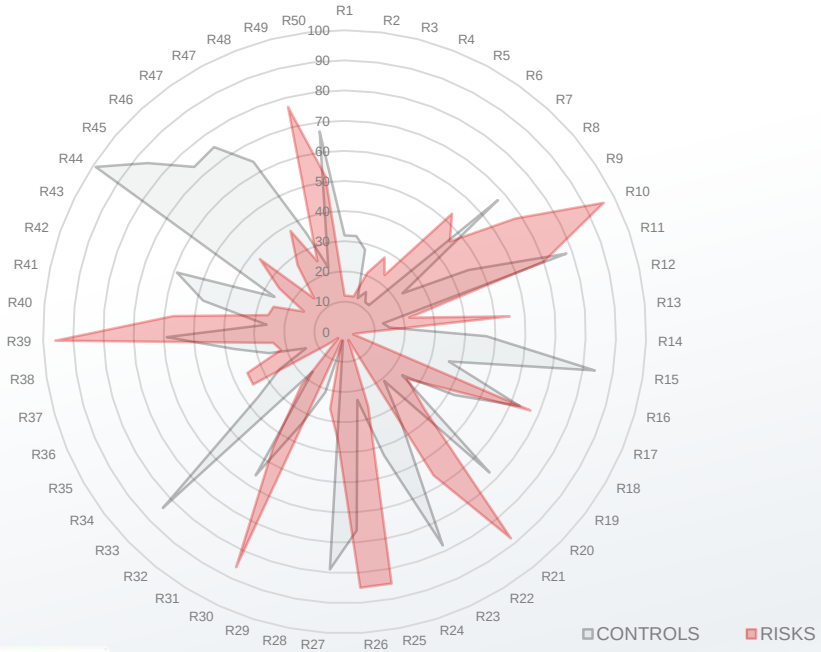
3. Risk Remediation Analysis

"Identifies security controls currently in place to mitigate threats and vulnerabilities."

Threat ID	Description	Controls	Risk Score	Asset #1		Asset #2		Asset #3	
				Potential Impact	Likelihood	Potential Impact	Likelihood	Potential Impact	Likelihood
T1	Description of cyber threat 1	Description of current controls	80%	5	4	5	4	5	4
T2	Description of cyber threat 2	Description of current controls	60%	5	3	5	3	5	3
T3									
T4									
T5									
T6									
T7									
T8									
T9									
T10									
T11									
...Tn									
Aggregate susceptibility									

4. Gap Analysis

"Identifies gaps between existing risk state and an organisations target risk profile "



For your top identified risks:

- Do your controls meet your needs?
- Have you under-invested in specific areas?
- Have you overspent in other areas?

5. Strategy & Planning

"Provides strategy recommendations based on findings, prioritising and aligning against business risk profile"

Schedule

ACTIVITY	Description	Duration
1. Crown Jewels	Workshop & Interviews	2 days on-site
2. Threat Susceptibility		
3. Risk Remediation	Gathering of data & evidence	Completion within 2 weeks after completion of workshops and interview *
4. Gap Analysis	Analysis	
5. Strategy & Planning	Evaluation	*Iff all data and evidence readily available

InfosecPartners
CYBERSECURITY

Thank you

Francisco Ordillano. Consulting Partner, Commercial Director

+44 207 193 4618 | francisco.ordillano@infosecpartners.com